

NDB
F. #2018R01655

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF (I)
A BLACK SAMSUNG CELLULAR
TELEPHONE, IMEI NUMBER
354805091516207, (II) A BLACK
SAMSUNG CELLULAR TELEPHONE,
IMEI NUMBER 355355111683834, (III) A
PINK SAMSUNG CELLULAR
TELEPHONE, IMEI NUMBER
355420092321448, AND (IV) A BLACK
IPAD, SERIAL NUMBER
DLXXKAT2K7M9, CURRENTLY
LOCATED IN THE EASTERN DISTRICT
OF NEW YORK

**APPLICATION FOR A
SEARCH WARRANT FOR
ELECTRONIC DEVICES**

Case No. 22-MJ-401

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, JOSEPH KANG, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”) since 2018. I am part of a Human Trafficking Task Force with HSI and New York City Police Department (“NYPD”). I have

experience investigating cases relating to human trafficking (including prostitution and other forced labor), violations of the Travel Act, alien smuggling, visa fraud and other immigration-related offenses and money laundering. As part of this work, I have experience executing search warrants on premises, vehicles and electronic devices.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is (i) a black Samsung cellular telephone, IMEI number 354805091516207, (ii) a black Samsung cellular telephone, IMEI number 355355111683834, (iii) a pink Samsung cellular telephone, IMEI number 355420092321448, and (iv) a black iPad, serial number DLXXKAT2K7M9, hereinafter collectively the “Devices.” The Devices are currently located in the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. Since approximately July 2018, HSI has been investigating Zhenai Li and others known and unknown in connection with a network of illicit massage parlors that operate under the guise of massage parlors in Queens, New York, and elsewhere, (the “Silk Spa network”) regarding possible violations of the Subject Offenses.

7. On or about March 8, 2022, the Honorable Marcia M. Henry, United States Magistrate Judge for the Eastern District of New York, issued an arrest warrant for Li charging her with 18 U.S.C. § 1952(a)(3)(A) (use of an interstate facility to promote prostitution). See 22-MJ-262 (MMH). The affidavit submitted in support of the complaint and arrest warrant is attached and incorporated herein.

8. On or about March 10, 2022, law enforcement officers executed Li's arrest at her residence in Queens, New York. After being informed of her arrest, the undersigned asked Li, in Korean, for consent to search the apartment, which she voluntarily agreed to grant. The undersigned also interpreted a consent to search and seize form from English to Korean for Li, which form Li reviewed and voluntarily signed.

9. Agents then searched the apartment and seized, among other things, the Devices and documents, including mail and receipts, related to Silk Spa 56 as that term is defined in the complaint supporting the arrest warrant for Li as well as other Silk Spa network locations.

10. As discussed in greater detail in the incorporated complaint, Li and her co-conspirators use electronic devices in furtherance of the Subject Offenses.

11. The Devices are currently in the lawful possession of HSI. They came into the HSI's possession incident to arrest and with consent. Therefore, while the HSI might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

12. The Devices are currently in the Eastern District of New York. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the HSI.

TECHNICAL TERMS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved

in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. Based on my training, experience, and research, and from consulting the manufacturers’ advertisements and product technical specifications available online I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA, tablet and internet-accessing device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed

via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the

application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to facilitate prostitution, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.


18. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not

involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

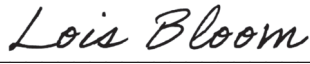
19. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



JOSEPH KANG
Special Agent
U.S. Department of Homeland Security
Homeland Security Investigations

Subscribed and sworn to before me
on April 7, 2022:



HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is (i) a black Samsung cellular telephone, IMEI number 354805091516207, (ii) a black Samsung cellular telephone, IMEI number 355355111683834, (iii) a pink Samsung cellular telephone, IMEI number 355420092321448, and (iv) a black iPad, serial number DLXXKAT2K7M9, hereinafter collectively the “Devices.” The Devices are currently located in the Eastern District of New York.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. § 1952(a)(3)(A) (use of an interstate facility to promote prostitution), 18 U.S.C. § 1952(a)(1)(A) (distribution of the proceeds of prostitution), 18 U.S.C. § 1956(h) (money laundering conspiracy) and 18 U.S.C. §§ 371 and 2422(a) (interstate prostitution conspiracy) (collectively, the “Subject Offenses”), and involve Zhenai Li and/or any co-conspirators since January 2018, including:

- a. lists of customers and related identifying information;
- b. communications with co-conspirators and customers and related identifying information;
- c. information regarding or reflecting Zhenai Li and/or any co-conspirator’s schedule or travel;
- d. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.